# 最良の符号を用いた新量子暗号の安全性評価のための信頼性関数の応用

情報科学科　吉田 真菜　　指導教員：臼田 毅

## 1　はじめに

鍵の有無により可能な量子測定が異なることを安全性に利用した量子暗号原理として KCQ (Keyed Communication in Quantum noise) があり，対応する量子暗号方式は KCQ プロトコルと呼ばれる [1]．本論文では，量子利得を用いてその安全性評価を行う．正規送受信者が鍵を共有しているのに対し，盗聴者はその鍵を持たない．よって，正規受信者が量子最適受信機を利用できるのに対し，盗聴者は最高でも古典最適受信機を用いることしかできない．この能力差が安全性を確立している．

先行研究として，特定の線形符号を対象にし量子利得評価をしたもの [2]，最良の符号による量子利得評価を行うため古典信頼性関数の上下界及び量子信頼性関数の上界を用いたもの [3] がある．しかし，量子信頼性関数の下界 [4] が用いられなかったため [3] の結果の精度は明らかではなかった．本論文では，この下界も用いることで，より厳密に量子利得評価を行う．

## 2　信頼性関数

本論文では，2 元符号で符号化された複素振幅 $\alpha$ の BPSK(Binary Phase Shift Keying) コヒーレント状態信号を扱う．信頼性関数 $E(R)$ は十分に長い符号長 $n$ と与えられた符号化率 $R$ において，復号誤り率を最小とする最良の符号を用いたときの復号誤り率 $P_{\mathrm{e}}^{\mathrm{opt}}(n,R)$ の指数のことである．

$$P_{\mathrm{e}}^{\mathrm{opt}}(n,R) = e^{-nE(R)} \tag{1}$$

信頼性関数を実際に求めることは困難であるが，その上下界は導出可能である．上下界が一致する場合は正確な信頼性関数の値が得られる．量子，古典ともに上界では，後述する $s$ の最適化の範囲が 0 以上，下界では $0 \le s \le 1$ である．

### 2.1　量子信頼性関数の上下界

量子信号の生起確率を $\xi$ とし，$\rho$ を各量子信号をその生起確率で混合した密度作用素とする．このとき，量子信頼性関数の上下界は以下のようになる．前述の通り，$s$ の最大化の範囲により上界か下界かが変わる．

$$\mu(s,\xi) = -\ln \mathrm{Tr}\rho^{1+s} \tag{2}$$

$$E_{\mathrm{Q}}(R) = \max_{s}\max_{\xi}\left[\mu(s,\xi) - sR\right] \tag{3}$$

### 2.2　古典信頼性関数の上下界

古典信頼性関数の上下界は，通信路入出力を $i$，$j$，元数 $M = M'$(本稿では 2)，生起確率 $\xi$ として以下のように表される．

$$\nu(s,\xi) = -\ln \sum_{j=1}^{M'}\left(\sum_{i=1}^{M}\xi_i P(j|i)^{\frac{1}{1+s}}\right)^{1+s} \tag{4}$$

$$E_{\mathrm{C}}(R) = \max_{s}\max_{\xi}\left[\nu(s,\xi) - sR\right] \tag{5}$$

## 3　量子利得

KCQ プロトコルの安全性評価は，量子最適受信機による誤り率が古典最適受信機による誤り率と比べてどれだけ優れているのかを示す “量子利得” と深く関わっている．

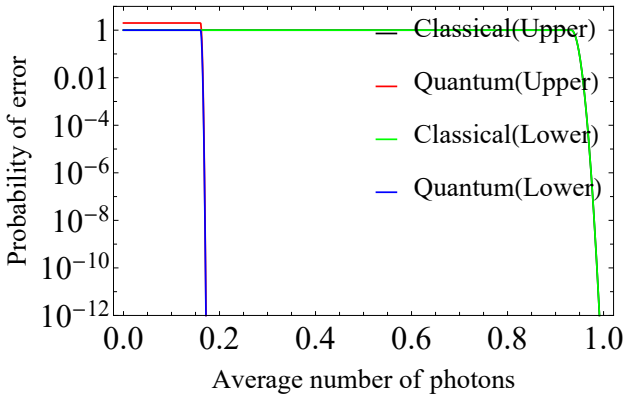


図 1　符号化率 $R$=0.4，符号長 $n = 10^5$ の誤り率．

上界評価手法 [1] は，盗聴者が古典最適受信機で測定した後に盗聴者に仮想的に鍵を開示するという解析手法である．測定後に鍵の全情報を知った盗聴者の能力は，実際の盗聴者の能力に比べ明らかに上界となる．この手法により，先の量子利得は正規受信者と盗聴者の能力差の下界となる．量子利得は，ある誤り率 $P$ を達成する量子の場合の平均光子数 $N_{\mathrm{s}}^{\mathrm{Q}}$ と古典の場合の平均光子数 $N_{\mathrm{s}}^{\mathrm{C}}$ を用いて以下のように表される．

$$\mathrm{Gain} = 10\log_{10}\frac{N_{\mathrm{s}}^{\mathrm{C}}(\mathrm{When}\ P_{\mathrm{C}} = P)}{N_{\mathrm{s}}^{\mathrm{Q}}(\mathrm{When}\ P_{\mathrm{Q}} = P)}\quad [\mathrm{dB}] \tag{6}$$

本論文では，符号化率 $R = 0.3, 0.5$，符号長 $n = 10000$ の場合，及び $R = 0.4$，$n = 10000$，$15000$，$20000$，$10^5$ の場合の量子利得を導いた．いずれの場合も量子信頼性関数の上下界は一致しなかったが，極めて近い値を取り，上下界がきついことがわかった．$R = 0.4$，$n = 10^5$ の場合の誤り率と平均光子数のグラフを図 1 に示す．$P = 10^{-12}$ の場合の量子利得は，その上下界から 7.614[dB] と 7.617[dB] の間であり，3 桁の精度で量子利得を算出することができた．

## 4　まとめ

本研究では，古典及び量子信頼性関数の上下界を用い，文献 [3] では下界評価のみであった量子利得を 3 桁の精度で明らかにした．しかしながら，符号長の増大に伴う量子利得の劇的な増加は得られなかった．これは通常の量子通信と KCQ プロトコルでは，最良の符号が異なるためと考えられる．今後，KCQ プロトコルに適した符号のクラスを明らかにしたい．

## 参考文献

[1] H.P. Yuen, arXiv:quant-ph/0311061v6, (2004).
[2] A. Kadoya, et al., Proc. of AQIS2015, pp.161-162, (2015).
[3] 和田他, H29 電気・電子・情報関係学会東海支部大会, (2017).
[4] M. Dalai, IEEE Trans. IT, **59**, pp.8027-8056, (2013).

## 公表論文

1. **吉田真菜**，松本直也，臼田毅，平成 30 年度電気・電子・情報関係学会東海支部連合大会，J3-4，(2018).
2. **吉田真菜**，和田えみり，宇佐見庄五，臼田毅， 第 41 回情報理論とその応用シンポジウム, pp.232-236, (2018).